1969

Numerical properties of the full transformation semigroup on a finite domain.

Sweeney, Orval Lester

Monterey, California. U.S. Naval Postgraduate School

NUMERICAL PROPERTIES OF THE FULL TRANSFORMATION SEMIGROUP ON A FINITE DOMAIN

by

Orval Lester Sweeney

United States
Naval Postgraduate School

THESIS

NUMERICAL PROPERTIES OF THE FULL TRANSFORMATION SEMIGROUP ON A FINITE DOMAIN

by

Orval Lester Sweeney

June 1969

Numerical Properties of the Full Transformation Semigroup on a Finite Domain

by

Orval Lester Sweeney
Lieutenant (junior grade), United States Navy
B.S., United States Naval Academy, 1968

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 1969

ABSTRACT

In this paper certain properties that are common to all finite transformation semigroups are discussed. For example special properties of ideals in transformation semigroups are established. It is also proved that every element of a finite transformation semigroup must be one-to-one from some maximal subset of its domain onto that same set. This maximal subset is decomposed into cycles, and results are obtained connecting the orders of the cycles of an element and the order of the monogenic semigroup generated by that element. Numerical results concerning arbitrary subsemigroups in the transformation semigroup on three elements are listed at the end of the paper.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The author would like to thank Professor C. O. Wilde for his helpful suggestions in preparing this paper.

I. INTRODUCTION

This paper is concerned with a specific class of semigroups, those consisting of all functions from a given finite set into that same set, the operation being functional composition. One reason for interest in the class of finite transformation semigroups is that, as will be shown, any finite semigroup can be embedded into transformation semigroups of suitable orders. Certain properties that are common to semigroups of this class will be discussed. Ideals with special properties will be singled out. Transformation semigroups will be decomposed into their monogenic subsemigroups. In addition, in an attempt to shed some light on the larger problem of finding the number of subsemigroups of arbitrary order in the full transformation semigroup on n elements, numerical results digitally computed for T_3, the transformation semigroup on three elements, will be listed.

II. SOME BASIC PROPERTIES OF TRANSFORMATION SEMIGROUPS

A full transformation semigroup is the collection of all functions on a certain fixed domain, with ranges contained in the same set; only the case of a finite domain will be considered here. The use of all functions on the same domain will insure closure under the operation of functional composition.

Notation. For a given positive integer n we denote the set of all functions from a fixed domain of n elements into itself by T_n.

The transformation semigroup T_n will be shown to be independent of the underlying set. For convenience, the domain, denoted R_n, will be taken to be $\{1,2,\ldots,n\}$. Then T_n will contain n^n elements. For arbitrary n, under the operation of functional composition, T_n is a semigroup, since the composite of two functions on the same domain is again a function on that domain, and associativity can be easily checked.

Note. If $u,v\varepsilon T_n$, then the composite of u and v, denoted $u\circ v$, is that function for which, if $i\varepsilon R_n$, $u\circ v(i) = v(u(i))$.

Proposition. If A is any set of order n, let S_n be the set of all functions on A into itself; then S_n is isomorphic to T_n.

Proof. Let η be any 1-1 function from R_n onto A, and define $\rho : T_n \to S_n$ by the following: if $u\varepsilon T_n$, define $\rho(u)$ to be that function in S_n which takes $\eta(i)$ to $\eta(u(i))$, for

$i = 1,2,\ldots,n$. This is easily shown to be a 1-1 mapping from T_n onto S_n, and the choice of domain is limited only to cardinality. From now on we will deal only with domain R_n.

Theorem 1. The transformation semigroup T_n is isomorphic to the set of all n-tuples with entries being positive integers from 1 to n, under the operation

$$(i_1,i_2,\ldots,i_n)\circ(j_1,j_2,\ldots,j_n) = (j_{i_1},j_{i_2},\ldots,j_{i_n}),$$

with equality component-wise.

Proof. Denote the above set of n-tuples by R^n. Define the function $\eta: T_n \to R^n$, where $\eta(u) = (u(1),u(2),\ldots,u(n))$. Since functional equality is defined component-wise, η is a 1-1 function. Since T_n and R^n both have order n^n, we need only show that η preserves the operation. If $u,v \in T_n$, then

$$\begin{aligned}\eta(u)\circ\eta(v) &= (u(1),u(2),\ldots,u(n))\circ(v(1),v(2),\ldots,v(n))\\ &= (v(u(1)),v(u(2)),\ldots,v(u(n)))\\ &= (u\circ v(1),u\circ v(2),\ldots,u\circ v(n))\\ &= \eta(u\circ v).\end{aligned}$$

Henceforth T_n and R_n will be used interchangeably. The significance of this representation of T_n is the ease with which multiplication may be performed, and the compact way in which it exhibits all of the functional values. An example of this multiplication procedure, in T_3, is given graphically below. The first component of the composite function is the component of the right-hand function which is indicated by the first component of the left-hand function, and so on for the second and third components of the composite function.

$$(2,3,1) \circ (3,1,3) = (1,3,3)$$

The question naturally arises as to the possibility of embedding S, an arbitrary finite semigroup of order n, into T_m, for some positive integer m. Since T_m appears to have m "degrees of freedom," it is natural to conjecture that S can be embedded into T_n, but this is not always possible.

Example. Let $S = \{x_1, x_2, x_3\}$, where multiplication is defined by $x_i x_j = x_i$. Assume $\rho\colon S \to T_3$ is 1-1 and preserves the semigroup operation. Then $\rho(x_i) \circ \rho(x_j) = \rho(x_i)$, or $\rho(x_j)[\rho(x_i)(k)] = \rho(x_i)(k)$, for $k = 1,2,3$. Hence $\rho(x_j)$ fixes every element in $R[\rho(x_i)]$, the range of $\rho(x_i)$, and $R[\rho(x_i)] \subseteq R[\rho(x_j)]$. Similarly, $R[\rho(x_j)] \subseteq R[\rho(x_i)]$, and $\rho(x_i)$ fixes each point in $R[\rho(x_j)]$. Hence $R[\rho(x_i)] = R[\rho(x_j)]$, for $i,j = 1,2,3$. Let $R = R[\rho(x_i)]$ for $i = 1,2,3$. Then for $k \varepsilon R$, $\rho(x_i)(k) = k$. If R contains three elements, then $\rho(x_i)$ is the identity for each i, which contradicts the assumption that ρ is 1-1. If R contains two elements, then there are only two ways to map the other element, and so only two distinct functions are possible, again a contradiction. If R contains one element then there is only one distinct function possible. Hence S cannot be embedded into T_3 isomorphically.

One might next hope that, by including anti-isomorphisms with the isomorphisms, any semigroup of order n could be embedded into T_n. This is an open question, and is certainly borne out in the above

example, where S is anti-isomorphic to the semigroup of all of the constant functions in T_3. In any case, it is possible to embed any semigroup of order n into T_{n+1}, as the next theorem states.

<u>Theorem 2</u>. Any finite semigroup of order n can be embedded into T_{n+1}.

Proof. Let $S_n = \{x_1,x_2,\ldots,x_n\}$ be any semigroup of order n. We must exhibit a 1-1 function from S_n into T_{n+1} which preserves the semigroup operation. Let s be the subscript function; i.e., $s(x_i) = i$ for $i = 1,2,\ldots,n$. Define $\rho\colon S_n \to T_{n+1}$ by $\rho(x_i) = (s(x_1x_i),s(x_2x_i),\ldots,s(x_nx_i),i)$. Since distinct elements from S_n map to functions with different evaluations at the point $n+1$, ρ is a 1-1 function. If $x_i,x_j \in S$, then

$$\begin{aligned}\rho(x_i)\circ\rho(x_j) &= (s(x_1x_i),\ldots,s(x_nx_i),i)\circ(s(x_1x_j),\ldots,s(x_nx_j),j)\\ &= (s(x_{s(x_1x_i)}x_j),\ldots,s(x_{s(x_nx_i)}x_j),s(x_ix_j)).\end{aligned}$$

But $x_{s(x_kx_d)} = x_kx_d$, since $s(x_{s(x_kx_d)}) = s(x_kx_d)$, and the subscript function is 1-1. Hence

$$\begin{aligned}\rho(x_i)\circ\rho(x_j) &= (s((x_1x_i)x_j),\ldots,s((x_nx_i)x_j),s(x_ix_j))\\ &= \rho(x_ix_j).\end{aligned}$$

<u>Theorem 3</u>. T_n can be embedded into T_{n+1}.

Proof. Let $\rho(i_1,i_2,\ldots,i_n) = (i_1,i_2,\ldots,i_n,n+1)$.

<u>Corollary 1</u>. Any semigroup of order n can be embedded into T_m for $m \geq n+1$.

Proof. It is easy to show by induction that T_{n+1} can be embedded into T_m for $m \geq n+1$. Since any semigroup of order n can be embedded into T_{n+1}, the composite of the two embeddings is the desired embedding.

Corollary 2. There are at least $n+1$ embeddings of T_n into T_{n+1}.

Proof. Let $S = \{1,2,\ldots,n+1\} \sim \{i'\}$, where i' is an integer between 1 and $n+1$. Let S_n be the transformation semigroup of all functions from S into S; then S_n is isomorphic to T_n. If $u \varepsilon S_n$, let $\rho(u)$ be defined by

$$\rho(u)(i) = \begin{cases} u(i) & \text{if } i \quad S \\ i' & \text{if } i = i' \end{cases}$$

Then, if $u,v \varepsilon S_n$, $u = v$ iff $\rho(u) = \rho(v)$, so that ρ is a 1-1 function. If $i \varepsilon S$, then

$$\rho(u) \circ \rho(v)(i) = \rho(v)[\rho(u)(i)] = \rho(v)(u(i)).$$

Since $u \varepsilon S_n \Rightarrow u(S) \subseteq S$, we have $u(i) \varepsilon S$, and $\rho(v)(u(i)) = \rho(u \circ v)(i)$. Hence ρ embeds S_n into T_{n+1}. Since there are $n+1$ choices of i', there are at least $n+1$ distinct embeddings.

Corollary 3. There are at least $\binom{n}{i}$ distinct embeddings of T_i into T_n, where $1 \leq i \leq n$.

Proof. There are $\binom{n}{i}$ ways to choose sets of order i from R_n, and we may embed the transformation semigroup on each set of order i into T_n in the same manner as before, fixing the $n - i$ elements not in the domain of the set generating T_i in the same manner as i' was a fixed point before. These $\binom{n}{i}$ embeddings of T_i into T_n are evidently all possible intersections of i of the images of the n embeddings of T_{n-1} into T_n .

III. IDEALS IN TRANSFORMATION SEMIGROUPS

The concepts of left, right, and two-sided ideals in a semigroup are well known. It is easy to show that for any n there exists a strictly decreasing sequence of two-sided ideals, $\{I_n, I_{n-1}, \ldots, I_1\}$, in T_n. It can also be shown that I_1, the set of all constant functions, is the smallest right ideal and the smallest two-sided ideal. Although there is no smallest left ideal, it will be shown that there are precisely n minimal left ideals, each constant function being a minimal left ideal.

Proposition. Let I_i be the set of all functions in T_n which contain at most i elements in their ranges, for $i = 1,2,3,\ldots,n$. Then $\{I_n, I_{n-1}, \ldots, I_1\}$ is a strictly decreasing sequence of two-sided ideals, with I_1 being the set of all constant functions.

Proof. Let $u \varepsilon I_i$. Then u has range containing at most i elements. Let $v \varepsilon T_n$. Then $u \circ v$ has at most i elements in its range, since $R[u \circ v] = u \circ v(R_n) = v(u(R_n))$, where $w(R_n) = R[w]$ is the range of w for any $w \varepsilon T_n$. The function v can map a set of at most i elements onto at most i elements. The function $v \circ u$ has at most i elements in its range, since $v \circ u(R_n) = u(v(R_n)) \subseteq u(R_n)$. Hence I_i is a two-sided ideal for each i. The sequence is obviously strictly decreasing, and I_1 is the set of all constant functions.

Theorem 4. The set of all constant functions in T_n, I_1, is the smallest right ideal and the smallest two-sided ideal in T_n.

Proof. Let I be a two-sided ideal in T_n. Let $v \varepsilon I_1$, and let $u \varepsilon I$. Then, for $i \varepsilon R_n$, $u \circ v(i) = v(u(i)) = v(i)$, since v is a constant function. Hence, $u \circ v = v$, and $I_1 \subseteq I$, since I is a right ideal. Since I_1 is a two-sided ideal, it must then be the smallest two-sided ideal. A similar argument also applies to any right ideal.

<u>Theorem 5</u>. In T_n, there are precisely n minimal left ideals, namely the singleton sets of elements of I_1.

Proof. Let $u \varepsilon T_n$, $v \varepsilon I_1$. Then $u \circ v = v$. Hence $\{v\}$ is a left ideal, and certainly minimal, since it contains only one element of T_n. We must show that every minimal left ideal in T_n is of this form. Let I be a minimal left ideal, and let $u \varepsilon I_1$, $v \varepsilon I$. Then $u \circ v \varepsilon I$. But $u \circ v(R_n) = v(u(R_n))$, and $u(R_n)$ consists of exactly one element. Hence $u \circ v(R_n)$ consists of precisely one element, and $u \circ v$ must be a constant function. Since $u \circ v$ is then a left ideal contained in I, $\{u \circ v\}$ must equal I, since I is minimal.

Since the above arguments concerning ideals in T_n do not involve finiteness, the results are true in general; i.e., if T_A is the semigroup of all functions from A into A, where A is a set with any cardinality, then the set of all constant functions, I_1, is the smallest right ideal and the smallest two-sided ideal in T_A. Similarly, the singleton sets of elements of I_1 are precisely the minimal left ideals, and $\{I_1, I_2, \ldots.\}$ is a sequence of strictly increasing two-sided ideals, where I_i is the set of all functions in T_A with range containing at most i elements.

IV. STRUCTURE THEOREMS FOR TRANSFORMATION SEMIGROUPS

In this section we will study numerical questions concerning monogenic subsemigroups in T_n. The simplest monogenic subsemigroup in T_n is, of course, the idempotent element.

Definition. A monogenic semigroup is a semigroup which is generated by one element.

Lemma. If $u \varepsilon T_n$, then u is an idempotent iff every point in the range of u is a fixed point of u.

Proof. Let u be an idempotent, and let $i \varepsilon R[u]$, the range of u. Then there exists $j \varepsilon R_n$ such that $u(j) = i$. Then $u^2(j) = u(j) = u(u(j))$. Hence $u(i) = i$. Now assume that u fixes every point in its range. Let $i \varepsilon R_n$. Then $u(i) \varepsilon R[u]$, so that $u(i)$ is a fixed point of u. Hence $u(u(i)) = u(i) = u^2(i)$, and u is an idempotent since i was arbitrary.

Theorem 6. There are exactly $\sum_{i=1}^{n} i^{n-i} \binom{n}{i}$ idempotents in T_n.

Proof. Consider all idempotents u with range consisting of i elements, where $1 \leq i \leq n$. There are $\binom{n}{i}$ ways to choose the range of u, and each element not in the range can be mapped to any element in the range. Hence for each i, there are $\binom{n}{i} i^{n-i}$ idempotents.

In order to obtain results for more general monogenic subsemigroups of T_n, we need some preliminary results, which are contained in the next three lemmas.

Lemma 1. For every $u \varepsilon T_n$ there exists $R \subseteq R_n$ for which u_R is 1-1 onto R, where u_R is the restriction of u to the set R.

Proof. Consider the set $\{1,u(1),\ldots,u^n(1)\}$. Since R_n contains n elements, there must be a repetition in this set, so assume $u^k(1) = u^p(1)$. Define $u^0(1)$ to be 1. Without loss of generality, assume $0 \leq k < p \leq n$, where p is chosen so that $p-k$ is minimized with respect to the restriction $u^k(1) = u^p(1)$. Let $R = \{u^k(1),u^{k+1}(1),\ldots,u^{p-1}(1)\}$; then u_R is 1-1 onto R.

Lemma 2. If u_R is 1-1 onto R, where u_R is as in lemma 1, and $p \varepsilon R$, then there exists a positive integer k such that $u^k(p) = p$.

Proof. Since u_R is, in particular, into R, we have $u^q(p) \varepsilon R$ for every positive integer p. Consider the set $\{p,u(p),\ldots,u^n(p)\}$. Let j be the smallest positive integer such that $u^j(p)$ is repeated in this set. We must show $j = 0$, so assume $j \neq 0$. Choose r so that $r - j$ is minimized with respect to the restriction $u^r(p) = u^j(p)$. Then $u(u^{j-1}(p)) = u^r(p)$ and $u(u^{r-1}(p)) = u^r(p)$. But $u^{j-1}(p) \neq u^{r-1}(p)$, since j is the smallest positive integer such that $u^j(p)$ is repeated. This contradicts the fact that u_R is 1-1 onto R. So $j = 0$, and there exists a k for which $u^k(p) = p$.

Lemma 3. If u_R is 1-1 onto R and for every $i \not\varepsilon R$ there exists a positive integer k_i such that $u^{k_i}(i) \varepsilon R$, then R must be the largest subset of R_n with the property that u_R is 1-1 onto R. Specifically, any other subset of R_n with that property must be contained in R.

Proof. Assume R is not the largest, but satisfies the hypotheses; i.e., assume $u_{R'}$ is 1-1 onto R' but $R \not\subset R'$. Then there exists an $i \varepsilon R \sim R'$. Let k_i be the smallest positive integer

such that $u^{k_i}(i)\varepsilon R$. Let $p = u^{k_i}(i)$. Then, by lemma 1, there exists a positive integer p_i such that $u^{p_i}(p) = p$. Then $u(u^{p_i-1}(p)) = p$. But $u(u^{k_i-1}(i)) = p$, where $u^{k_i-1}(i) \neq u^{p_i-1}(p)$, since $u^{k_i-1}(i)\not\varepsilon R$, and $u^{p_i-1}(p)\varepsilon R$. But $u^{k_i-1}(i)\varepsilon R'$, and $u^{p_i-1}(p)\varepsilon R'$, since $i\varepsilon R$, and $u^{p_i-1}(p) = u^{k_i+p_i-1}(i)$. This contradicts the fact that $u_{R'}$ is 1-1 onto R'.

Theorem 7. Any $u\varepsilon T_n$ is 1-1 onto a largest subset of R_n; i.e., there exists a set $R_{max}\subseteq R_n$ such that $u_{R_{max}}$, the restriction of u to R_{max}, is 1-1 onto R_{max} and every other subset D of R_n upon which u is 1-1 onto D is contained in R_{max}.

Proof. By lemma 1, for any u there exists an $R_1\subseteq R_n$ such that u is 1-1 onto R_1. If there exists an $i\varepsilon R_1$ such that $u^k(i)$ is not in R_1 for any positive integer k, let p be the smallest positive integer such that $u^p(i)$ is repeated. Then let k be such that $k - p$ is minimized subject to the restriction $u^p(i) = u^k(i)$. Let $R_2 = \{u^p(i),u^{p+1}(i),\ldots,u^{k-1}(i)\}$. Then u_{R_2} is 1-1 from R_2 onto R_2, and R_1 and R_2 are disjoint, since i generates R_2 and $u^k(i)\not\varepsilon R_1$ for every positive integer k. Hence $u_{R_1\cup R_2}$ is 1-1 onto itself. This process may be continued, obtaining a terminating sequence of disjoint subsets of R_n, say $\{R_1,R_2,\ldots,R_m\}$, where for every $i\not\varepsilon\bigcup_{j=1}^{m}R_j$ there exists a positive integer k_i such that $u^{k_i}(i)\varepsilon\bigcup_{j=1}^{m}R_j$, and the restriction of the function u to this union is 1-1 onto this union. Hence, by lemma 3, $\bigcup_{j=1}^{m}R_j$ is the maximal subset of R_n upon which u is 1-1 onto.

Notation. For a specific $u\varepsilon T_n$, R^u_{max} is the maximal subset of R_n upon which u is 1-1 onto that same subset.

Definition. For $u \varepsilon T_n$, if k is the smallest integer such that $u^k(i) = i$, then i is said to be in a k-cycle, or a cycle of order k. Let j be the smallest integer in the set $\{i, u(i), \ldots, u^{k-1}(i)\}$. Then $(j, u(j), \ldots, u^{k-1}(j))$ is said to be the cycle which contains i.

Corollary to Theorem 7. For $u \varepsilon T_n$, R^u_{max} may be decomposed uniquely into cycles.

Proof. The existence of the decomposition was established in the proof of Theorem 7. Uniqueness is easy to prove, for all cycles must be disjoint, since the restriction of an element in T_n to one of its cycles is 1-1, and if $i \varepsilon R^u_{max}$, then i determines a unique cycle.

Definition. If $u \varepsilon T_n$, then $i \varepsilon R_n$ is called a generator if it does not have a preimage.

It is evident that no element of a cycle may be a generator.

Definition. The element $i \varepsilon R_n$ is a generator of order k if i is a generator and $u^k(i) \not\varepsilon R^u_{max}$ but $u^{k-1}(i) \varepsilon R^u_{max}$.

V. SOME COMBINATORIAL PROBLEMS IN TRANSFORMATION SEMIGROUPS

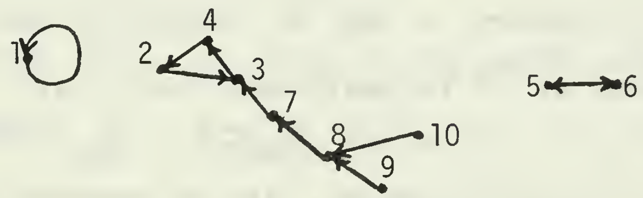
The connection will now be made between transformation semigroups and graph theory. This connection will aid in solving combinatorial problems in transformation semigroups.

Definition. i. If i is a generator of u of order k, then $(i,u(i),\ldots,u^{k-1}(i))$ is called a path.

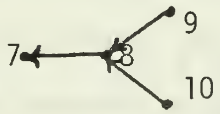
ii. A tree is the collection of all paths that intersect a given path.

Hence the 1-1 correspondence between the elements of T_n and the collection of all labeled directed graphs of order n (with the restriction that only one directed line may emanate from a point) now becomes readily apparent.

As an example, in T_{10}, let $u = (1,3,4,2,6,5,3,7,8,8,)$. The structure of u is illustrated diagrammatically as follows.



Here (1), $(2,3,4)$, $(5,6)$ are cycles, and $\{(9,8,7),(10,8,7)\}$ is the only tree (see diagram below).



Lemma 1. In T_n, $u^{k+1} = u$ if an only if the order of every cycle in u divides k and every generator is of order one.

Proof. Let $u^{k+1} = u$. Then, for every $i \varepsilon R_n$, $u^k(u(i)) = u(i)$, so that $u(i)$ is in some cycle for every i, and therefore is in R_{max}; hence every generator is of order one. Now let i be in some cycle. Then $u(i)$ is in the same cycle. Let the cycle be of order q. Then $q \leq k$, since if $q > k$, then $u^k(u(i)) \neq u(i)$. By the division algorithm, $k = qs + r$, where $0 \leq r < q$, and $s \geq 0$, since $q < k$. Now $u^k(u(i)) = u^{qs+r}(u(i)) = u^r(u^{qs}(u(i)))$. But $u^q(u(i)) = u(i)$, so that, after repeated application, we obtain $u^r(u(i)) = u^k(u(i))$. Hence, to satisfy the hypothesis, $r = 0$, and q divides k.

Now suppose that the order of every cycle of u divides k, and let every generator in u be of order one. Then for every $i \varepsilon R_n$, $u(i)$ must be in some cycle. Let the cycle be of order q, where $qs = k$. Then $u^k(u(i)) = u^{qs}(u(i)) = u^{q(s-1)}(u(i))$, since $u(i)$ is in a cycle of order q. Hence, by repeated application again, we obtain $u^k(u(i)) = u(i)$.

It is desirable to obtain the number of elements in T_n such that $u^{k+1} = u$, for arbitrary n and k. Toward this end k should be factored into all of its positive divisors, say $1 = q_1, q_2, \ldots, q_m = k$. For a given set $R^u_{max} \subseteq R_n$, R^u_{max} should be decomposed into all possible subsets, with the restriction that each subset must have order q_i for some i such that $1 \leq i \leq m$. Each collection of subsets would then be the cyclic decomposition of R^u_{max} for a certain element u of T_n such that $u^{k+1} = u$. All possible cyclic decompositions would be obtained by finding all possible collections of such subsets.

As an example, for $k = p$, a prime less than or equal to n, for R^u_{max} containing i elements, where $1 \leq i \leq n$, there could be

no p-cycles and i fixed points (cycles of order one), or anywhere from 1 to i_p p-cycles (with remainder of R^u_{max} being fixed points), where i_p is the greatest integer less than or equal to i/p. If there are q p-cycles and $i - pq$ fixed points, then there are

$$\frac{n!}{(n-i)!\,(p!)^q\,(i-pq)!} \quad \text{ways to choose these elements}$$

from R_n. There are $(p - 1)!$ ways to arrange each group of p elements into a p-cycle, since the first element must be the smallest element from the group, and the other $p - 1$ elements may appear in any order. Each of the $n - i$ elements not in R^u_{max} can map to any given element in R^u_{max}, since the only restriction on a generator is that it be of order one. Hence, if the order of R^u_{max} is i, we obtain

$$\sum_{q=0}^{i_p} \frac{n!\,(p-1)!^{\,q}\,i^{n-i}}{(n-i)!\,(p!)^q\,(i-pq)!} \quad \text{elements } u \text{ in } T_n \text{ with}$$

the property $u^{p+1} = u$. Since i can assume values from 1 to n, we obtain

$$\begin{aligned}
\#\{u \varepsilon T_n :\, u^{p+1} = u\} &= \sum_{i=1}^{n} \sum_{q=0}^{i} \frac{n!\quad i^{n-i}}{(n-i)!\,p^q\,(i-pq)!} \\
&= \sum_{i=1}^{n} \frac{n!\,i^{n-i}}{(n-i)!} \left[\sum_{q=0}^{i_p} \frac{1}{p^q\,(i-pq)!} \right]
\end{aligned}$$

where $\#\{u\varepsilon T_n :\, u^{p+1} = u\}$ is the cardinality of the set $\{u\varepsilon T_n :\, u^{p+1} = u\}$.

It is obvious that in T_n, $\#\{u\epsilon T_n\colon u^{p+1} = u\}$ is the number of idempotents in T_n if p is a prime greater than n.

For k not a prime $\#\{u\epsilon T_n\colon u^{k+1} = u\}$ is not so easy to calculate. A formula will be developed in conjunction with an algorithm to calculate $\#\{u\epsilon T_n\colon u^{k+1} = u\}$ for any k. In T_n, for a fixed positive integer k, N_j^i is the number of distinct ways that i elements from R_n may be arranged as combinations of cycles of any or all of the following orders: $\{q_1,q_2,\ldots,q_m\}$, where $1 = q_1<q_2<\ldots<q_m = k$ are the positive divisors of k.

Lemma 2. In T_n, for any fixed positive integer k,

$$N_j^i = \sum_{s=0}^{i_j} N_{j-1}^{i-sq_j} \frac{i!}{q_j^s\,(i - sq_j)!}\ ,$$ where i_j is the greatest integer not exceeding i/q_j, for $i\geq j>1$. $N_1^i = 1$ for $i\geq 1$.

Proof. There is only one way for i elements to be arranged as 1-cycles, or fixed points so that $N_1^i = 1$ for any positive integer i. In calculating N_j^i, where $j>1$, let s be the number of q_j-cycles in the i elements. Then $0\leq s\leq i_j$. The s q_j-cycles may be arranged in $\dfrac{i!}{q_j^s\,(i - sq_j)!}$ ways, as has already been shown. The $i - sq_j$ remaining elements must then be arranged in cycles of orders q_r for $r<j$. The number of ways these elements may be arranged with these restrictions is $N_{j-1}^{i-sq_j}$. Since s takes on all integral values from 0 to i_j, the desired result is obtained by summing over all possible values of s.

It is evident that by the recursion relation exhibited in the preceding lemma, for any positive integer k, in T_n, the number N_m^i may be calculated.

Theorem 8. In T_n, for any positive integer k,

$$\#\{u\varepsilon T_n: u^{k+1} = u\} = \sum_{i=1}^{n} \binom{n}{i} N_m^i \, i^{n-i}.$$

Proof. Consider all elements in T_n for which the order of R_{max}^u (for that $u\varepsilon T_n$) is equal to i. By lemma 1, since every generator is of order one, each element in R_n not in R_{max}^u can map to any of the elements in R_{max}^u. There are $\binom{n}{i}$ ways to choose the elements in R_{max}^u. By lemma 1, the order of each cycle in R_{max}^u must divide k. N_m^i is then the number of ways R_{max}^u may be formed, for this particular i, by lemma 1. Since lemma 1 specifies the necessary and sufficient conditions for u^{k+1} to equal u in T_n, we have $\binom{n}{i} N_m^i \, i^{n-i}$ elements in T_n satisfying those conditions. Since i was arbitrary, the proof is complete.

Lemma. In T_n, if $u^{k+1} = u$ and $u^{q+1} = u$ for some $q<k$, then q divides k. Conversely, if $u^{q+1} = u$, where q divides k, then $u^{k+1} = u$.

Proof. Let $u^{q+1} = u$, where q divides k. Then $k = qp$ for some positive integer p. Hence $u^{k+1} = u^{qp+1} = u^{q+1}$, since u^q is an idempotent. Hence $u^{k+1} = u$. Now let $u^{k+1} = u^{q+1} = u$, where $q<k$. Without loss of generality, assume q is the smallest positive integer such that $u^{q+1} = u$. By the division algorithm, $k = qs + r$, where $s \geq 0$ and $0 \leq r < q$. Then $u^{k+1} = u^{qs+r+1} = u^{r+1}$. Since $r<q$ and q is the smallest positive integer such that $u^{q+1} = u$, we have $u^{k+1} = u$ iff $r = 0$, and hence q divides k.

Remark. We may now evaluate $\#\{u\varepsilon T_n: u^{k+1} = u;\ k$ the smallest such positive integer$\}$ by repeated application of the following recursion relation:

$$\#\{u\varepsilon T_n\colon u^{r+1} = u\} - \sum_{q=q_1}^{q_m} \#\left\{u\varepsilon T_n\colon u^{q+1} = u; \quad \begin{array}{l}q \text{ the smallest such}\\ \text{positive integer}\end{array}\right\}$$

$$= \#\left\{u\varepsilon T_n\colon u^{r+1} = u; \quad \begin{array}{l}r \text{ the smallest such}\\ \text{positive integer}\end{array}\right\} ,$$

where $\{q_1,q_2,\cdots,q_m\}$ are the positive divisors of r in ascending order.

<u>Lemma</u>. In T_n, if $u^{k+1} = u$, where k is the smallest such positive integer, and if q is a positive integer less than k, then u^q generates the same semigroup as u does iff q and k are relatively prime.

Proof. If $k>1$, then u^k cannot generate the semigroup generated by u, since u^k is an idempotent. The lemma is trivially satisfied if $k = 1$, so let $0<p<k$, and we show u^p generates $S = \{u,u^2,\ldots,u^k\}$ iff p and k are relatively prime. Let p and k be relatively prime, where $0<p<k$. Assume u^p does not generate S. Then two elements from the set $\{u^p,u^{2p},\ldots,u^{kq}\}$ must be equal, since this set is contained in S, and if all elements are distinct, it must equal S. Let $u^{ip} = u^{jp}$, where $1\leq j<i\leq k$. Then $u^{(k-i)p+1}\,u^{ip} = u^{(k-i)p+1}\,u^{jp}$

$$u^{kp+1} = u^{k+1} = u = u^{(k+(j-i))p+1}.$$

But $0<i-j<k \Rightarrow 0<k + (j-i)<k \Rightarrow p\leq(k + (j - i))p<kp$. But k and p are relatively prime, so that the least common multiple of k and p is kp. Since p divides $(k+ (j - i))p$, k cannot divide $(k + (j - i))p$. So by the division algorithm we obtain $(k + (j - i))p = kq + r$, where $0\leq q$ and $0<r<k$. Hence, returning to the equality obtained above, we have

$$u = u^{kq+r+1} = u^{kq+1}\circ u^r = u\circ u^r = u^{r+1}.$$

Since $0<r<k$, a contradiction is obtained.

Now assume u^p generates S, but p and k are not relatively prime. Let M be the least common multiple of k and p, and let D be the greatest common divisor. Then $pk = MD$, where $D>1$, since p and k are relatively prime. Then $u^{(k/D)p} = u^{k(p/D)} = u^k$, since u^k is an idempotent. Hence $u^M = u^k$, where $M<k$, and u^p cannot generate S.

Theorem 9. In T_n, the number of monogenic subsemigroups of the type $S = \{u,u^2,\ldots,u^k\}$, where $u^{k+1} = u$ and the elements of S are distinct, is

$$\frac{1}{p}\ \#\{u\varepsilon T_n\colon\ u^{k+1} = u;\ \ k \text{ the smallest such positive integer}\}\ ,$$

where p is the number of relatively prime integers less than k.

Proof. Since every semigroup of the above type has p elements which generate it, we need only divide the number of elements in T_n which generate such a semigroup by p.

Corollary. The number of monogenic subsemigroups of T_n which are of order p and of the form $\{u,u^2,\ldots,u^p\}$, where $u^{p+1} = u$ and p is a prime, is

$$\sum_{i=1}^{n}\ \sum_{q=1}^{i_p} \frac{n!\ i^{n-i}}{(n-i)!\ p^{q+1}\ (i - pq)!}\ .$$

A formula was not obtained for the number of monogenic subsemigroups of arbitrary type in T_n, namely the case where $u^{k+p} = u^p$, for $p>1$. However some results were obtained, and a sample of these results follows.

Lemma. In T_n, $u^{k+p} = u^p$ if and only if all cycles of u have order which divides k and all the generators of u are of order less than or equal to p.

Proof. Let $i \varepsilon R_n$. Then $u^{k+p}(i) = u^p(i)$, so that $u^p(i) \varepsilon R^u_{max}$, and if i is a generator it must have order less than or equal to p. If i is in a cycle, then $u^p(i)$ is in the cycle, and since $u^k(u^p(i)) = u^p(i)$, all cycles must have order which divides k by a previous argument (see Lemma 1 preceding Theorem 8). If all of the cycles of u have order which divides k, and all generators have order less than or equal to p, then, for any $i \varepsilon R_n$, $u^p(i)$ is in a cycle, and hence $u^k(u^p(i)) = u^p(i)$. Since i is arbitrary, we have $u^{k+p} = u^p$.

Definition. For any $u \varepsilon T_n$, the order of a tree is the maximum of the orders of the paths contained in that tree.

Theorem 10.

$$\#\{u \varepsilon T_n : u^{k+p} = u^p\} = \sum_{i=1}^{n} \binom{n}{i} N^i_m \sum_{j=1}^{n-1} T^i_j \, i^j ,$$

where T^i_j is the number of distinct ways j trees may be formed, of order less than or equal to p, from $n-i$ elements.

Proof. Let i be the order of R^u_{max}. There are $\binom{n}{i}$ ways to choose these elements from R_n, and N^i_m ways to form each i elements into a distinct collection of cycles which have order dividing k. There can be anywhere from 1 to $n-i$ trees, for each i, and the trees may map to any of the i elements in R^u_{max}. Hence, for any fixed i and j, there are $T^i_j \, i^j$ possible ways to form and map the elements not in R^u_{max}. By summing over i and j, the theorem is proved.

Note. The number T^i_j, used in this process, must be obtained by an exhaustive method.

No analytical results were obtained in the larger problem concerning all types of subsemigroups of T_n of a certain fixed order. However, numerical results digitally computed for T_3 appear below in a table.

NUMBER OF SUBSEMIGROUPS IN T_3

ORDER	WITH IDENTITY	TOTAL
1	1	10
2	12	45
3	37	86
4	55	136
5	87	192
6	119	197
7	96	186
8	96	144
9	64	109

BIBLIOGRAPHY

Clifford, A.H. and Preston, G.B., The Algebraic Theory of Semigroups, v. 1, p. 9-16, American Mathematical Society, 1961.

Denes, J., On Transformations, Transformation Semigroups, and Graphs, paper presented at the colloquium held at Tihany, Hungary, September, 1966, Theory of Graphs, edited by P. Erdos and G. Katona, p. 65-76, Academic Press, 1968.

Ljapin, E.S., Semigroups, p. 15-28, 106-112, American Mathematical Society, 1963.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Documentation Center Cameron Station Alexandria, Virginia 22314	20
2.	Library, Code 0212 Naval Postgraduate School Monterey, California 93940	2
3.	Naval Ship Systems Command, Code 2052 Department of the Navy Washington, D.C. 20370	1
4.	Professor C. O. Wilde, Code 53Wm Department of Mechanical Engineering Naval Postgraduate School Monterey, California 93940	1
5.	LTJG Orval L. Sweeney, USN 6903 Dartmouth Street College Park, Maryland 20740	1

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)* Naval Postgraduate School Monterey, California 93940	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP

3. REPORT TITLE

Numerical Properties of the Full Transformation Semigroup on a Finite Domain

4. DESCRIPTIVE NOTES *(Type of report and, inclusive dates)*

Master's Thesis

5. AUTHOR(S) *(First name, middle initial, last name)*

Orval Lester Sweeney

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
June 1969	29	3

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
b. PROJECT NO.	
c.	9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*
d.	

10. DISTRIBUTION STATEMENT

This document has been approved for public release and sale; its distribution is unlimited.

~~Distribution of this document is unlimited~~

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY Naval Postgraduate School Monterey, California 93940

13. ABSTRACT

In this paper certain properties that are common to all finite transformation semigroups are discussed. For example special properties of ideals in transformation semigroups are established. It is also proved that every element of a finite transformation semigroup must be one-to-one from some maximal subset of its domain onto that same set. This maximal subset is decomposed into cycles, and results are obtained connecting the orders of the cycles of an element and the order of the monogenic semigroup generated by that element. Numerical results concerning arbitrary subsemigroups in the transformation semigroup on three elements are listed at the end of the paper.

DD FORM 1 NOV 65 1473 (PAGE 1)

S/N 0101-807-6811

Security Classification

A-31408

Security Classification

14 KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Transformation						
Semigroups						

DD FORM 1 NOV 65 1473 (BACK)

S/N 0101-807-6821

Security Classification

A-31409